AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended) A wireless communication~~computing~~ apparatus having

a processor; and

a memory comprising computer executable instructions which, when executed are operative to:

facilitate login to a user account at a backup server, the user account associated with a user having the wireless communication apparatus and another computing device;

facilitate designation of data on the wireless ~~computing~~communication apparatus to backup;

generate a ~~strongly collision free deterministic identifier~~hash value for said data;

communicate said ~~strongly collision free deterministic identifier~~hash value to ~~a~~ the backup server to enable said backup server to determine whether said data is already available to said backup server or not; and

only if said backup server indicates that said data is not already available to said backup server, send said data to said backup server to enable the backup server to store the data and provide the data to the other computing device.

2. (Original) The apparatus of claim 1, wherein the apparatus further comprises a transceiver and audio input/output components coupled to the processor and memory.

3. (Original) The apparatus of claim 1 wherein said data is sent in compressed form to said backup server.

4. (Cancelled)

5. (Original) The apparatus of claim 4 wherein said hash value is generated by a cryptographic hashing algorithm.

6. (Original) The apparatus of claim 5 wherein said cryptographic hashing algorithm is selected from the group of cryptographic hashing algorithms consisting of: MD2, MD4, MD5, SHA, HAS160, HAVAL, RIPEMD (including RIPEMD-128/160/255/320), TIGER, Snefru, FFT-Hash I, FFT-Hash II, MAA, DSA, Cell hash, hash functions based on additive knapsacks, and hash functions based on multiplicative knapsacks.

7. (Currently Amended) The apparatus of claim 1 wherein said ~~strongly collision free deterministic identifier~~hash value is a cryptographic checksum.

8. (Currently Amended) The apparatus of claim 1 wherein said ~~strongly collision free deterministic identifier~~hash value is wirelessly communicated via a communication medium selected from the group consisting of: RF signals, optical signals, audio modulated signals, and electromagnetic signals.

9. (Currently amended) The apparatus of claim 1 further comprising designating a data type not to backup from the wireless ~~computing~~ communication apparatus.

10. (Currently amended) The apparatus of claim 1 further comprising designating a data location not to backup from the wireless ~~computing~~ communication apparatus.

11. (Currently Amended) A wireless ~~computing~~ communication apparatus having

a processor; and

a memory comprising computer executable instructions which, when executed are operative to:

select a backup compilation;

receive a ~~strongly collision free deterministic identifier~~hash value for restoration data from said backup compilation from a backup server; and

only if said ~~strongly collision free deterministic identifier~~hash value is not identical to any ~~strongly collision free deterministic identifier~~hash value of data currently on the wireless ~~computing~~communication apparatus, receive said restoration data from said backup server.

12. (Currently Amended) A ~~computer-implemented~~ method of backing up a wireless communication~~computing~~ device, the method comprising:

facilitating, by the wireless communication device login to a user account at a backup server, the user account associated with a user having the wireless communication device and another computing device;

facilitating, by the wireless communication device, designating data on the wireless communication~~computing~~ device to backup;

generating a ~~strongly collision free deterministic identifier~~hash value for said data;

communicating said ~~strongly collision free deterministic identifier~~hash value to ~~a~~ the backup server to enable said backup server to determine whether said data is already available to said backup server or not; and

only if said backup server indicates that said data is not already available to said backup server, sending said data to said backup server to enable the backup server to store the data and provide the data to the other computing device.

13. (Currently Amended) The method of claim 12 wherein said ~~strongly collision free deterministic identifier comprises a hash value of said data~~generating comprises generating the hash value using a cryptographic hashing algorithm.

14. (Currently amended) The method of claim 12 further comprising designating a data type not to backup from the wireless ~~computing~~communication device.

15. (Currently amended) The method of claim 12 further comprising designating a data location not to backup from the wireless ~~computing~~communication device.

16. (Currently Amended) A computer implemented method of restoring data to a wireless ~~computing~~communication device, the method comprising:

selecting a backup compilation;

receiving a ~~strongly collision-free deterministic identifier~~hash value for data from said backup compilation from a backup server; and

only if said ~~strongly collision-free deterministic identifier~~hash value is not identical to any ~~strongly collision-free deterministic identifier~~hash value of data on the wireless ~~computing~~communication device, receiving said data from said backup server.

17. (Currently Amended) A computing server apparatus having

a processor; and

a memory comprising computer executable instructions which, when executed are operative to:

receive a request to ~~backup~~ restore data ~~from~~ to a client device, including a ~~strongly collision-free deterministic identifier for said data~~selection of a backup compilation;

~~determine whether said identifier corresponds to backup data already on the server apparatus~~provide a hash value associated with the backup compilation to the client device to enable the client device to determine whether data from the backup compilation is already stored on the client device; and

only if said ~~identifier~~ hash value is not identical to any hash value of data on the client device~~does not correspond to previously backed-up data on the server apparatus~~, ~~receiving~~ providing said data from the backup compilation ~~from~~to said client device.

18. (Cancelled)

19. (Currently Amended) The apparatus of claim 17, wherein ~~further~~ said backup ~~data~~ compilation on the server apparatus was previously backed up from another client device, both client devices associated with a user account.